REMARKS

Claims 1-25 are pending in the present application. In the Office Action, claims 1, 3-5, 9-12, 15, 17-18, 20-22, and 25 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Quigley, et al (U.S. Patent No. 6,650,624). Claims 2 and 16 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Quigley in view of Fleming, et al (U.S. Patent No. 6,212,360). Claims 6 and 19 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Quigley in view of Weidner, et al (U.S. Patent No. 5,987,572). Claims 7-8 and 23-24 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Quigley in view of Bestock (U.S. Patent No. 5,363,449). Claims 13-14 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Quigley in view of Albrecht, et al (U.S. Patent No. 6,510,521). The Examiner's rejections are respectfully traversed.

Independent claim 1 sets forth, among other things, a standard mode driver to extract encrypted data from a digital received signal and a privileged mode driver for decrypting encrypted data, which includes one or more control codes. The decrypted control codes are provided to a physical layer hardware unit, which uses the decrypted control codes to configure assigned transmission parameters of the physical layer hardware unit. Independent claim 15 sets forth, among other things, receiving encrypted data over a communications channel in a standard processing mode of a processing unit and transitioning the processing unit into a privileged processing mode. Claim 15 also sets forth decrypting encrypted data in a privileged processing mode, extracting control codes from the decrypted data in the privileged processing mode, and transmitting an upstream signal over a communications channel based on transmission assignments defined by the control codes.

Applicants use a separate standard mode driver and a privileged mode driver to enhance security in a software implemented communication system, where standard drivers are susceptible to external tampering. Applicant defines privileged mode as "a mode of operation not visible to other processes, such as applications or drivers, executing on the computer 100" (page 13, lines 21-23). The Office Action asserts that Quigley teaches distinct privileged and standard operating modes. The Office Action cites Quigley at col. 24, line 59 – col. 25, line 5 as supporting this assertion. To the contrary, Quigley merely teaches receiving encrypted data and control codes and decrypting and extracting the data and control codes using a decryptor 344 and a DMA controller 312. The DAM controller 312 processes both the user data and the control codes. Neither of these processing entities switches modes of operation to prevent the control codes from being visible to the standard mode functionality. In fact, Quigley teaches operation in only a standard mode. Using a key unique to each user does not equate to operating in a privileged mode, as defined by Applicants. Applicants also use a unique key for each user to decrypt data, however, Applicants, unlike Quigley, perform that encryption in a privileged mode distinct from the standard mode. Quigley merely decrypts data in a standard mode of operation.

Another aspect that Quigley fails to teach or suggest is the use of **distinct drivers**. As set forth in claim 1, Applicants employ two different drivers -- a standard mode driver and a privileged mode driver to perform the communication functions. A driver is employed by a general purpose processing device and provides a link between the processing device and the controlled hardware. In contrast, Quigley uses dedicated hardware and firmware, and as such, does not employ drivers as they are commonly defined in the art.

For at least the aforementioned reasons, Applicants respectfully submit that the present invention is not anticipated by Quigley and request that the Examiner's rejections of claims 1, 3-5, 9-12, 15, 17-18, 20-22, and 25 under 35 U.S.C. 102(b) be withdrawn.

The dependent claims rejected by the Office Action are allowable for at least the reasons provided above. The cited references do not cure the defects identified above, and accordingly, it is respectfully submitted that the pending claims are not obvious in view of the prior art of record.
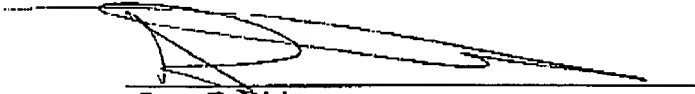
The dependent claims also include additional features that distinguish them from the art of record. Claims 9 and 21 include the additional feature of encrypting the control codes extracted from the previously decrypted data in the privileged mode, sending the encrypted control codes in the standard mode to the physical layer hardware. This encryption represents a second encryption distinct from the encryption previously performed on the incoming data. The incoming data is already encrypted. In the privileged mode, the data is decrypted, the control codes are extracted and then re-encrypted. The encrypted control codes are then sent in the standard mode to the physical layer hardware. Quigley simply decrypts the data and extracts the control codes in a single mode. Quigley does not re-encrypt the control codes at all, much less do so in a privileged mode, and subsequently send them in a standard mode in encrypted form to the physical layer device.

For at least the aforementioned reasons, Applicants respectfully submit that the present invention is not obvious over the prior art of record. Applicants respectfully request that the Examiner's rejections of claims 2, 6-8, 13-14, 16, 19, and 23-24 under 35 U.S.C. 103(a) be withdrawn.

For the aforementioned reasons, it is respectfully submitted that all claims pending in the present application are in condition for allowance. The Examiner is invited to contact the undersigned with any questions, comments or suggestions relating to the referenced patent application.

Respectfully submitted,

Date: 12/2/05

Scott F. Diring
Reg. No. 35,119
Williams Morgan & Amerson, P.C.
10333 Richmond Avenue, Suite 1100
Houston, TX 77042
(713) 934-7000
(713) 934-7011 (Fax)

ATTORNEY FOR APPLICANTS